

Amendments To Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (currently amended) A transponder-reader transaction system configured with a biometric security system, said system comprising:

a transponder configured to communicate with a reader;
a reader configured to communicate with said system;
a hand geometry scan sensor configured to detect a proffered hand geometry scan sample, said hand geometry scan sensor configured to communicate with said system; and,
a device configured to verify said proffered hand geometry scan sample to facilitate a transaction-; and,

wherein said system is configured to determine whether a user requested transaction exceeds a preloaded value defined by a preloaded value data file associated with a transponder; determine whether said transaction exceeds a combination of said preloaded value and a reload value defined by a reload protocol data file associated with said transponder, wherein said preloaded value data file and said reload protocol data file define predetermined values for use in satisfying a user transaction request; notify a user to proffer a biometric sample to authorize use of said combination of said preloaded value and said reload value to complete said transaction; detect a proffered biometric sample at a sensor communicating with said system; verify said proffered biometric sample; and authorize said transaction to proceed by applying said preloaded value from a first funding source associated with said transponder and applying a portion of said reload value from one of said first funding source and a second funding source according to said reload protocol data file.

2. (currently amended) The transponder-reader transaction system of claim 1, wherein said hand geometry scan sensor is configured to communicate with said system via at least one of a transponder, a reader, and a network.

Claims 3-7 (cancelled)

8. (original) The transponder-reader transaction system of claim 1, wherein said hand geometry scan sensor device is configured with at least one of an infrared optical sensor and a three-dimensional imaging system.

9. (currently amended) The transponder-reader transaction system of claim 1, wherein said hand geometry scan sensor is configured to detect and verify hand geometry scan characteristics including at least one of: blood flow, body heat, hand shape, finger length, finger thickness, and finger curvature.

10. (cancelled)

11. (currently amended) The transponder-reader transaction system of claim 1, further including at least one of: a third-party security vendor device and protocol/sequence controller a ~~device~~ configured to compare a proffered hand geometry scan sample with a stored hand geometry scan sample.

12. (cancelled)

13. (currently amended) The transponder-reader transaction system of claim 1 14, further comprising a device configured to compare said proffered hand geometry scan sample with a stored hand geometry sample, wherein a stored hand geometry scan sample comprises a registered hand geometry scan sample which is associated with at least one of: personal information, credit card information, debit card information, savings account information, and loyalty point information.

14. (cancelled)

15. (currently amended) The transponder-reader transaction system of claim 1 14, further comprising a device configured to compare said proffered hand geometry scan sample with a stored hand geometry sample, wherein a stored hand geometry scan sample comprises a registered hand geometry scan sample wherein different registered hand geometry scan samples are associated with a different one of: personal information, credit card information, debit card information, savings account information, and loyalty point information.

16. (currently amended) The transponder-reader transaction system of claim 1 14, wherein a said hand geometry scan sample is primarily associated with at least one of: first user information, wherein said first information comprises personal information, credit card

information, debit card information, savings account information, and loyalty point information, and wherein a hand geometry scan sample is secondarily associated with at least one of second user information, wherein said second information comprises personal information, credit card information, debit card information, savings account information, and loyalty point information, where second user information is different than first user information.

17. (cancelled)

18. (original) The transponder-reader transaction system of claim 1, wherein said transponder is configured to deactivate upon rejection of said proffered hand geometry scan sample.

19. (currently amended) The transponder-reader transaction system of claim 1, wherein said hand geometry scan sensor is configured to provide a notification upon detection of a sample.

20. (cancelled)

21. (original) The transponder-reader transaction system of claim 1, wherein said device configured to verify is configured to facilitate the use of at least one secondary security procedure.

22. (currently amended) A method for facilitating biometric security in a transponder-reader transaction system comprising:

proffering a hand geometry scan to a hand geometry scan sensor communicating with said system to initiate verification of a hand geometry scan sample for facilitating authorization of a transaction, wherein said authorization comprises:

determining whether a user requested transaction exceeds a preloaded value defined by a preloaded value data file associated with a transponder;

determining whether said transaction exceeds a combination of said preloaded value and a reload value defined by a reload protocol data file associated with said transponder, wherein said preloaded value data file and said reload protocol data file define predetermined values for use in satisfying a user transaction request;

notifying a user to proffer a hand geometry scan sample to authorize use of said combination of said preloaded value and said reload value to complete said transaction;

detecting said proffered hand geometry scan sample at a sensor communicating with said system;

verify said proffered hand geometry scan sample;

authorizing said transaction to proceed by applying said preloaded value from a first funding source associated with said transponder; and,

applying a portion of said reload value from one of said first funding source and a second funding source according to said reload protocol data file.

Claims 23-24 (cancelled)

25. (original) The method of claim 22, wherein said step of proffering includes proffering a hand geometry scan to at least one of an infrared optical sensor and a three-dimensional imaging system.

Claims 26-29 (cancelled)

30. (currently amended) The method of claim 22 29, wherein said step of comparing includes comparing hand geometry scan characteristics including at least one of: blood flow, body heat, hand shape, finger length, finger thickness, and finger curvature.

Claims 31-33 (cancelled)

34. (currently amended) A method for facilitating biometric security in a transponder-reader transaction system comprising:

determining whether a user requested transaction exceeds a preloaded value defined by a preloaded value data file associated with a transponder;

determining whether said transaction exceeds a combination of said preloaded value and a reload value defined by a reload protocol data file associated with said transponder, wherein said preloaded value data file and said reload protocol data file define predetermined values for use in satisfying a user transaction request;

notifying a user to proffer a hand geometry scan sample to authorize use of said combination of said preloaded value and said reload value to complete said transaction;

detecting a said proffered hand geometry scan sample at a sensor communicating with said system to obtain a proffered hand geometry scan sample;

verify ~~the~~ said proffered hand geometry scan sample;

authorizing a said transaction to proceed upon verification of the proffered hand geometry scan sample by applying said preloaded value from a first funding source associated with said transponder; and,

applying a portion of said reload value from one of said first funding source and a second funding source according to said reload protocol data file.

35. (cancelled)

36. (original) The method of claim 34, wherein said step of detecting a proffered hand geometry scan includes detecting a proffered hand geometry scan at least one of an infrared optical sensor and a three-dimensional imaging system.

Claims 37-41 (cancelled)

42. (currently amended) The method of claim 34, wherein said step of verifying includes comparing a proffered hand geometry scan sample with a stored hand geometry scan sample by comparing hand geometry scan characteristic including at least one of: blood flow, body heat, hand shape, finger length, finger thickness, and finger curvature.

Claims 43-46 (cancelled)

47. (new) The transponder-reader transaction system of claim 1, further comprising said reader configured to provide a first radio frequency (RF) interrogation signal for powering a transponder system, to receive a transponder system RF signal, and to communicate transponder system account data related to said transponder system RF signal to a merchant system, said reader including, a first interrogator for providing said first RF interrogation signal; said transponder system authentication circuit comprising a reader authentication circuit in communication with said first interrogator for authenticating said transponder system RF signal; an RFID reader database for storing RFID reader data, said reader database in communication with said reader authentication circuit; an RFID reader protocol/sequence controller in communication with at least one of said first interrogator, said reader authentication circuit, and said reader database, said reader protocol/sequence controller configured to facilitate control of an order of operation of said first interrogator, said reader authentication circuit, and said reader database; and an RFID reader communications interface configured to communicate with said merchant system, said reader communications interface configured to provide said transponder

system account data, wherein said transponder system is configured to receive said first RF interrogation signal, to authenticate said first RF interrogation signal, and to transmit said transponder system account data, said transponder system further comprising: a first transponder responsive to said first RF interrogation signal; a transponder system authentication circuit in communication with said first transponder, said transponder system authentication circuit configured to authenticate said first RF interrogation signal; a transponder system database for storing said transponder system account data, said transponder system database in communication with said transponder system authentication circuit; and a transponder system protocol/sequence controller in communication with at least one of said first transponder, said transponder system authentication circuit, and said transponder system database, said transponder system protocol/sequence controller configured to control the order of operation of said first transponder, said transponder system authentication circuit, and said transponder system database, wherein said transponder system protocol/sequence controller is configured to activate said transponder system authentication circuit in response to said first RF interrogation signal having an RFID reader authentication code, said transponder system authentication circuit configured to encrypt said reader authentication code to provide an encrypted RFID reader authentication code, said transponder system authentication circuit configured to provide said encrypted RFID reader authentication code to said first transponder for providing to said reader, wherein said reader is configured to receive said encrypted RFID reader authentication code, and wherein said reader protocol/sequence controller is configured to activate said reader authentication circuit in response to said encrypted RFID reader authentication code, wherein said reader database is configured to provide a transponder system decryption security key to said reader authentication circuit in response to said encrypted RFID reader authentication code, said transponder system decryption security key for use in decrypting said encrypted RFID reader authentication code to form a decrypted RFID reader authentication code, said transponder system decryption security key provided to said reader based on an unique transponder identification code, wherein said reader authentication circuit is configured to compare said decrypted RFID reader authentication code and said reader authentication code to determine whether a match exists, and wherein said reader protocol/sequence controller is configured to activate said reader communications interface where said reader authentication

circuit matches said decrypted RFID reader authentication code and said reader authentication code.

48. (new) The transponder-reader transaction system according to claim 47, wherein said transponder system protocol/sequence controller activates said transponder system authentication circuit in response to said first RF interrogation signal, wherein said transponder system authentication circuit is configured to provide a transponder authentication code to said first transponder for providing to said reader.

49. (new) The transponder-reader transaction system according to claim 48, wherein said reader authentication circuit is configured to receive said transponder authentication code, said reader protocol/sequence controller activating said reader authentication circuit in response to said transponder authentication code, said reader authentication circuit configured to encrypt said transponder authentication code to form an encrypted transponder authentication code, wherein said reader is configured to provide said encrypted transponder authentication code to said transponder system.

50. (new) The transponder-reader transaction system according to claim 49, wherein said transponder system database is configured to store at least one of a transponder system identification data and an RFID reader decryption security key, and wherein said transponder system database is configured to provide said reader decryption security key to said transponder system authentication circuit in response to said encrypted transponder authentication code, said reader decryption security key for use in decrypting said encrypted transponder authentication code to form a decrypted transponder authentication code.

51. (new) The transponder-reader transaction system according to claim 50, wherein said transponder system authentication circuit is configured to compare said decrypted transponder authentication code and said transponder authentication code to determine whether a match exists.

52. (new) The transponder-reader transaction system according to claim 51, wherein said transponder system account data is in magnetic stripe format.

53. (new) The transponder-reader transaction system according to claim 52, wherein said transponder system account data is encrypted as a pre-encrypted transponder system account

data, wherein said transponder system database is configured to provide said pre-encrypted transponder system account data to said reader when said transponder system authentication circuit matches said decrypted transponder authentication code and said transponder authentication code.

54. (new) The transponder-reader transaction system according to claim 53, wherein said reader communications interface is configured to provide a transponder system PIN and said pre-encrypted transponder system account data when said transponder authentication code matches said decrypted transponder authentication code, and said decrypted RFID reader authentication code matches said reader authentication code.

55. (new) The transponder-reader transaction system of claim 1, wherein said system is further configured to update said preloaded value data file according to said reload protocol data file.

56. (new) The transponder-reader transaction system of claim 1, wherein said system is further configured to provide a transponder system identifier and update reload indicia to a user interface to obtain user authorization prior to reloading said preloaded value.

57. (new) The transponder-reader transaction system of claim 1, wherein said system is further configured to provide incentives to a transponder user based on said reloading of said preloaded value.

58. (new) The transponder-reader transaction system of claim 1, wherein said system is further configured to provide a transponder system identifier to an issuer system server and providing in real-time an update reload protocol to said issuer system server for reloading the preloaded value in real-time according to said reload protocol.